METHODS AND APPARATUS FOR PROVIDING NETWORKED CRYPTOGRAPHIC DEVICES RESILIENT TO CAPTURE

Abstract

Techniques are provided by which a device that performs private key operations (e.g., signatures or decryptions) in networked applications, and whose local private key is activated with, for example, a password or PIN, can be immunized to offline dictionary attacks in case the device is captured. The techniques do not assume tamper resistance of the device, but rather exploit the networked nature of the device, in that the device's private key operations are performed using a simple interaction with a remote server. This server, however, is untrusted, i.e., its compromise does not reduce the security of the device's private key unless the device is also captured, and need not have a prior relationship with the device. Techniques are also provided for supporting key disabling, by which the rightful owner of a stolen device can disable the device's private key even if the attacker already knows the user's password.